DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology
Office of Information Security
Risk Management and Incident Response
Incident Resolution Team

Monthly Report to Congress of Data Incidents

September 30 - November 3, 2013

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000095262	Mishandled/ Misused Physical or Verbal Information	VISN 08 Orlando, FL	9/30/2013	10/11/2013	

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0597449	9/30/2013	INC000000317112	N/A	N/A	N/A		1

Incident Summary

Veteran A was given Veteran B's medication list when Veteran A visited the pharmacy for pick-up. The medication list also showed two future appointments for Veteran B. Unfortunately, Veteran A covered up Veteran B's name with a sticky note so we are unable to verify name and extent of any SSN information. It appears there is a date at the top of the list, but it is not flagged as a DOB. The Privacy Officer (PO) will contact Veteran A today to determine the name of Veteran B and if any SSN was under the sticky note. Veteran A used the list to buttress a Congressional complaint regarding his medications in general, which was how the facility learned of the error. Veteran A will be contacted to ascertain the Veteran B's name and what, if any SSN info was covered by the sticky note.

Incident Update

09/30/13:
The medication list was returned to the facility PO on 10/01/13 by mail. Upon examination, the PO confirmed that no SSN was printed. However, a MM-DD-YYYY was machine printed across the top of the form, but not flagged as a DOB. Besides listing three medications, the form also listed two future appointments by date and clinic name.

10/03/13:
Veteran B will be sent a notification letter.

Resolution

Pharmacists cautioned to exercise more caution when handing paperwork to Veterans. This same message is being passed to all pharmacy staff.

DBCT

No DBCT decision needed. This is a representative ticket. There were a total of 104 Mis-Handling incidents this reporting period. Because of repetition, the other 103 are not included in this report, but are included in the "Mis-Handling Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000095275	Mishandled/ Misused Physical or Verbal Information	VISN 23 Des Moines, IA	9/30/2013	10/22/2013	

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0597461	9/30/2013	INC000000317157	N/A	N/A	N/A		5

Incident Summary

An outside agency reported receiving five other Veterans' paperwork along with one of their requests. The paperwork included the Veterans' full name, address, last four digits of social security number and service connection information for means tests. The agency shredded the information they received after reporting it.

Incident Update

09/30/13:
Five Veterans will be sent a general notification letter.

Resolution

The Supervisor took action today to re-educated staff to review closely before sending out. They need to more than just thumb through the papers going out.

DBCT

No DBCT decision needed. This is a representative ticket. There were a total of 120 Mis-Mailed incidents this reporting period. Because of repetition, the other 119 are not included in this report, but are included in the "Mis-Mailed Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000095421	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Charleston, SC	10/2/2013	10/16/2013	

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0597631	10/2/2013	INC000000317738	N/A	No	N/A		1

Incident Summary

Patient A received a prescription intended for Patient B. Patient B's name and type of medication was compromised. Patient A reported the incident to the Salisbury VA Medical Center (station 659) and a replacement has been requested for Patient B. Charleston Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a CMOP packing error. The CMOP employees will be counseled and retrained in proper packing procedures.

Incident Update

10/03/13:
Patient B will receive a HIPAA letter of notification.

Resolution

The CMOP employees were counseled and retrained in proper packing procedures.

DBCT

No DBCT decision needed. This is a representative ticket. There were a total of 14 Mis-Mailed CMOP incidents out of 7,665,866 total packages (11,511,471 total prescriptions) mailed out for this reporting period. Because of repetition, the other 13 are not included in this report, but are included in the "Mis-Mailed CMOP Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000095639	Mishandled/ Misused Physical or Verbal Information	VISN 02 Syracuse, NY	10/8/2013		

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0597838	10/8/2013	INC000000318777	N/A	N/A	N/A	1	64

Incident Summary

A Home Health Provider reported to the Privacy Officer (PO) that he lost the Home Care Agenda that contained the name and last four digits of the SSN on discharged patients, new admissions and those under 90-day review. No medical information was included on this list. He reported that he also lost a non-VA discharge instruction sheet that was pending his review. This contained the patient's name, date of birth, medications and procedures done. The PO will be investigating further to determine if the provider has an authorization to transport protected health information (PHI) on file as the provider stated he is required to take PHI off site to do his job. The PO educated the provider on the requirement to transport any personally identifiable information (PII) in a special attention envelope so it is properly secured when taking off site.

Incident Update

10/21/13:
Sixty-Four patients will receive notification letters. One patient will receive a letter offering credit protection services due to full name and date of birth being exposed.

DBCT

No DBCT decision needed. This is informational due to the number of Veterans affected.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000096347	Missing/Stolen Equipment	VISN 12 Milwaukee, WI	10/29/2013	11/5/2013	11/5/2013

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0598534	10/29/2013	INC000000323050	N/A	N/A	N/A		

Incident Summary

An inventory review of IT assets was completed at the Zablocki VA Medical Center. Below are the results for the Lost/Unable to Locate VA IT Equipment:

Computer Laptops - 2
Computer PCs - 11

All IT assets are loaded with the Guardian Edge encryption software. All equipment that leaves the facility is encrypted.

Incident Update

11/04/13:
These items were determined to be missing as a result of an IT Equipment Inventory, No data breach occurred as all devices were encrypted.

Resolution

VA Police have conducted their investigation and Reports of Survey were completed. No data breach occurred.

DBCT

No DBCT decision needed. This is a representative ticket. There were a total of 4 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 3 are not included in this report, but are included in the "IT Equipment Inventory Incidents" count at the end of this report.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000096350	Mishandled/ Misused Physical or Verbal Information	VISN 22 Las Vegas, NV	10/29/2013		11/5/2013

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0598558	10/30/2013	INC000000323348	N/A	N/A	N/A		73

Incident Summary

Two possible privacy violations were discovered by the Privacy Officer (PO) on 10/29/13. #1 Site Manager was given travel dispute documentation by a Veteran that included a listing of Mental Health Group names. The Veteran claims that the VA Mental Health Provider gave him the listing containing 28 Veteran names and last 4 SSN for the dispute. #2 In answer to a Congressional Inquiry not related to a privacy issue, attached to the complaint were three pages that looked like Mental Health sign in sheets, possibly given to Veteran by the same VA Mental Health Provider. Listings include the names and last 4 SSN of 45 Veterans. The PO is investigating to determine if the VA Mental Health Provider or staff member gave personally identifiable information (PII) to the Veterans.

Incident Update

10/31/13
Seventy-three Veterans will receive a notification letter.

DBCT

No DBCT decision needed. This is informational due to number of Veterans affected.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000096384	Missing/Stolen Equipment	WASHINGTON DC-VACO - 101 Washington, DC	10/30/2013	10/31/2013	11/5/2013

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0598569	10/30/2013	INC000000323321	N/A	N/A	N/A		

Incident Summary

VA Property Management Division is reporting the loss of a Compaq CPU for February 2013.

Incident Update

10/31/13:
The CPU was a desktop computer. It was an old computer that was used to track equipment. No employees were mapped to the CPU. No employees ever logged into the CPU using a Personal Identity Verification (PIV) card or used any personally identifiable information (PII).

Resolution

The Information Security Officer (ISO) reminded employee to report lost equipment in a timely fashion.

DBCT

No DBCT decision was needed. This is informational due to missing equipment.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000096509	Unauthorized Electronic Access	VISN 20 Walla Walla, WA	11/1/2013		11/5/2013

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0598684	11/1/2013	INC000000323956	N/A	N/A	N/A	1519	

Incident Summary

An employee emailed the wrong spreadsheet with protected health information (PHI) of full name and full SSN to an external agency unencrypted.

Incident Update

11/04/13:
The email was erroneously sent to the National Acupuncture Detoxification Association, which is a training and advocacy organization. The nurse attended a class to become certified with this agency. The person has been instructed to delete the email and also delete the deleted folder of their email. In addition she courtesy copied this same spreadsheet to the Nurse Recruiter at the VA in Salt Lake City. He responded that he had not opened the attachment and he deleted the email. The nurse did not intend to send a spreadsheet. She intended to send a file that was verification of a credential that she holds. She has applied for a position at the Salt Lake City VA and the nurse recruiter there asked for the credential.

The spreadsheet included 1522 Veterans' name, full SSN, a column for date of service and name of the provider that the Veteran is enrolled to. The name of spreadsheet is "Check log flu." The people on the list received an influenza vaccine from a non-VA source such as a Walgreens, this is what we call a "historical" vaccine. In Infection Control, we add the historical vaccine to the number of vaccines administered at the VA to come up with an immunization rate.

11/05/13:
The VA position is for a newly created position --Holistic RN. They are looking for an RN with certification in complementary or alternative medicine. She was asked to provide a copy of the credential from the National Acupuncture Detoxification Association (NADA), but she had not retained a copy of the credential. She asked NADA if they could email her the credential and they did so. She went to send the credential on to the VA and a cc to NADA in case the VA had questions and that is when she accidentally attached a spreadsheet and not the credential.

The recipient opened the email and immediately responded to the nurse that the wrong attachment had been sent. The recipient did not print the email. The recipient did delete the email. The recipient wrote an email saying they had deleted the email and deleted the deleted email box.

11/06/13:
The final count is 1519 due to the removal of duplicates.

DBCT **DBCT Decision Date:** 11/5/2013

11/05/13:
The DBCT reviewed and concurred that this is a data breach. This is a HITECH incident, requiring credit protection services and a press release. The Privacy Officer is working on them and is on target to meet the 60 day timeframe for notification.

Total number of Internal Un-encrypted E-mail Incidents	89
Total number of Mis-Handling Incidents	104
Total number of Mis-Mailed Incidents	120
Total number of Mis-Mailed CMOP Incidents	14
Total number of IT Equipment Inventory Incidents	4
Total number of Missing/Stolen PC Incidents	3
Total number of Missing/Stolen Laptop Incidents	10 (10 encrypted)
Total number of Lost BlackBerry Incidents	19
Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents	1